Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual Section 64.2009(e) CPNI Certification for 2012 covering the prior calendar year 2011

1. Date filed: 2/29/2012

2. Name of company covered by this certification: CSINet Internet Access Corp.

3. Form 499 Filer ID: [New]

4. Name of signatory: Douglas M. Konieczny

5. Title of signatory: President/CEO

6. Certification:

I, Douglas M. Konieczny, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____. President/CEO

Attachments: Accompanying Statement explaining CPNI procedures

CPNI Policy Statement

1. Our company utilizes an employee training program with a disciplinary process and supervisory review to ensure compliance with CPNI rules and regulations.

2. All of the company's proprietary data bases, including that containing customer information, are password protected, and access to same is limited to authorized personnel only. Distribution of the password is limited to those authorized personnel. The password will be changed routinely, and whenever an employee with access to such data bases leaves the company.

3. No customer information in any form is to be removed from the company's offices by employees or others. This includes computer printouts, handwritten information or notes, copies of files or documents in any electronic form, and verbal transmission of customer information to persons who are not direct employees of the company.

4. Employees are to closely guard customer lists, contact information, telephone numbers, and all other customer information, both proprietary and public, to prevent any information from being removed from our offices by non-employees either accidentally or intentionally.

5. Disconnected or inactive customer files are to be retained for no more than 3 years, and then shredded. Disconnected or inactive customer files are never to be placed in the trash unshredded. Customer database printouts are to be shredded when replaced by newer printouts.

6. Our company has a supervisory approval process in place for any proposed outbound marketing request for CPNI.

7. Our company has a notification process in place to alert law enforcement, the FCC and affected customers in the event of a CPNI breach.

8. Our company requires a photographic identification from any customers requesting account information in our retail stores. Our company has a mechanism whereby customers can access their accounts online. Should a customer forget their online account password, the password will be sent to the customer's previously supplied email address on file. Our company requires that all requests for CPNI that come in by telephone be reduced to writing and sent to the Company via e-mail or paper, so no CPNI is released to customers on the telephone. Responses to customer inquiries are sent to the customer's address of record or previously-supplied e-mail account.

9. Among other things, any online access system will include a notification process to provide immediate notice to customers when a customer-initiated password or backup for forgotten passwords, an online account, or the address of record, is created or changed.

10. Our company has a formal process in place to certify the CPNI protection policies

instituted by our applicable vendors, service bureaus and wholesale carriers. Our company does not conduct joint marketing with these entities and therefore is not required to obtain opt-in consent from customers for joint marketing purposes.

11. Appropriate disciplinary action will be taken for any violations of this policy.